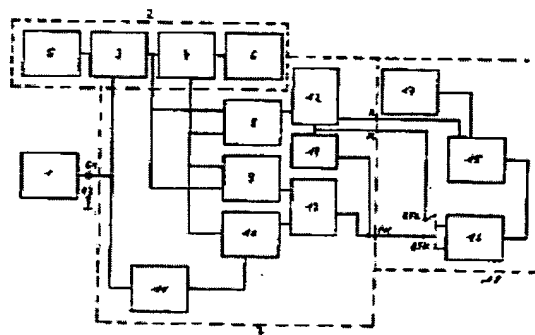


AG
Docket #4657
INV.: T. Mann et al.**Electronic security switching network**

Patent number: DE4422296
Publication date: 1994-11-17
Inventor: ORLOWSKI STEFFEN (DE)
Applicant: EMATEC ORLOWSKI & PARTNER (DE)
Classification:
- international: E05B47/00; E05B49/00; B60R25/00
- european: B60R25/00, G07C9/00E14B
Application number: DE19944422296 19940625
Priority number(s): DE19944422296 19940625

Abstract of DE4422296

The invention relates to an electronic security switching network having a key-like encoder (1), a plug holder (21), a code comparator (2), code recognition logic (7) and an output stage (18) having switches (15; 16) for the opening or commissioning function. The encoder has a clock frequency. The data transmission is carried out via the operating voltage supply lines of the encoder. The code comparator comprises an address comparator (3) and a data comparator (4) as well as memories (5; 6) assigned thereto. The code recognition logic recognises not only the correct code but also incorrect codes in a digital and analog manner, the latter being more likely to be recognised. An enable switch (15) of the output stage is actuated in the case of a correct code and an inhibit switch (16) in the case of incorrect codes. The two switches act in the opposite direction in the circuits to be switched.



Data supplied from the esp@cenet database - Worldwide

USPS EXPRESS MAIL
EV 415 086 281 US
APRIL 15 2004

AG



①⑨ BUNDESREPUBLIK
DEUTSCHLAND



DEUTSCHES
PATENTAMT

⑫ Patentschrift
⑩ DE 44 22 296 C 2

⑤① Int. Cl. 6: 4657
E 05 B 47/00
E 05 B 49/00
B 60 R 25/00

⑳ Aktenzeichen: P 44 22 296.3-31
㉑ Anmeldetag: 25. 6. 94
㉒ Offenlegungstag: 17. 11. 94
㉓ Veröffentlichungstag
der Patenterteilung: 14. 9. 95

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

⑦③ Patentinhaber: Ematec Orlowski & Partner, 04736 Waldheim, DE	⑦② Erfinder: Orlowski, Steffen, 04720 Ziegra, DE
⑦④ Vertreter: Härtig, O., Dipl.-Ing., Pat.-Anw., 04209 Leipzig	⑤⑥ Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften: DE 29 28 913 B1 DE 33 42 651 A1 DE 29 11 160 A1 DE 27 26 737 A1

⑤④ Elektronisches Sicherheitsschaltnetzwerk

DE 44 22 296 C 2

DE 44 22 296 C 2

USPS EXPRESS MAIL
EV 415 086 281 US
APRIL 15 2004

Die Erfindung betrifft ein elektronisch codiertes Sicherheitsschaltnetzwerk für Öffnungs- oder Inbetriebnahmefunktionen an Gebäuden, Räumen, Anlagen, Geräten, Fahrzeugen u. ä.

Zum Schutz vor unbefugter Öffnung oder Inbetriebnahme gibt es eine Vielzahl mechanischer, elektrischer und elektronischer Sicherheitsvorkehrungen. Als ein wesentlicher Schritt zur Erhöhung der Sicherheit hat sich die Anwendung von elektronischen Schaltnetzwerken mit Codegebern und integrierten Codeempfängern erwiesen. Das Ziel aller Lösungen für derartige Schaltnetzwerke ist darauf gerichtet, das Kopieren der meist einen Codeleser erfordernden Codegeber, das Entschlüsseln des Codes und die Auslösung der Schaltfunktionen durch Manipulation zu erschweren bzw. unmöglich zu machen.

Bei einer bekannten Diebstahl-Sicherheitsvorrichtung für Kraftfahrzeuge (DE-OS 27 26 737) ist der Codegeber als Schlüssel ausgebildet und mit einer magnetischen oder optischen Codierung versehen. Beim Einstecken des Schlüssels in einen Codeleser überprüft ein Codevergleicher den Code des Codegebers mit dem gespeicherten Code. Stimmen die beiden Codes nicht überein, wird ein optischer und/oder akustischer Alarm ausgelöst und/oder eine Einrichtung des Fahrzeugs, wie z. B. der Anlasser oder die Zündung, unwirksam gemacht. Der gespeicherte Code ist unveränderlich. In der DE-OS 29 11 160 und der DE-OS 29 28 913 werden Diebstahl-Sicherheitsvorrichtungen für Fahrzeuge mit einem zweiteiligen Code beschrieben, der im ersten Fall einen veränderbaren Teilcode, im zweiten Fall zwei umspeicherbare Teilcode enthält. Diese Umcodierung muß natürlich für den Fahrzeugbesitzer leicht durchführbar sein, wodurch die Möglichkeiten für einen versierten Dieb, den Code zu entschlüsseln bzw. einen neuen Code entsprechend einem mechanisch paßfähigen Codegeber einzuspeichern, nicht gering sind. Zur weiteren Absicherung der erwünschten Schaltfunktionen verknüpft bei der Vorrichtung nach DE-PS 29 28 913 eine Logikschaltung das Ausgangssignal des Codevergleichers mit einem Freigabesignal des Codelesers bei richtig eingestecktem Codegeber. Sie besteht aus einem Negator und einem UND-Tor für ein Alarmsignal und drei UND-Toren sowie einem Flip-Flop für das Schaltsignal und seine Negation.

Bekannt ist schließlich noch ein Verfahren zur Absicherung des Zugriffs an Terminals, Räumen, Maschinen und Fahrzeugen (DE-OS 33 42 651), das nicht auf einem elektronischen Sicherheitsschaltnetzwerk fußt, sondern das Vorhandensein eines Rechners mit entsprechender Software voraussetzt. Das Verfahren sieht die Echtheitsprüfung von zwei voneinander unabhängigen Codes in zwei aufeinanderfolgenden Schritten vor, wobei der zweite, maschinell eingegebene Code erst nach Decodierung des ersten, als echt erkannten Identitätscodes des Benutzers geprüft wird. Ein derartiges Verfahren ist verhältnismäßig aufwendig und deshalb in vielen Anwendungsfällen nicht praktikierbar.

Die bekannten codierten Sicherheitsschaltnetzwerke enthalten keine direkte Feststellung von Falschcodes. Sie bieten deshalb keine ausreichende Sicherheit der Öffnungs- oder Inbetriebnahmefunktionen vor ihnen. Sie setzen eine ständige Präsenz des Codegebers im Codeleser voraus, um die einmal erfolgte Schaltfunktion aufrechtzuerhalten. Kontaktschwierigkeiten insbesondere bei der Codelesung können den Schaltzustand ge-

fährden, weil sie einen Falschcode vortäuschen. Die Codeabastung bzw. -lesung ist taktunabhängig. Damit fehlt eine Hürde für die unbefugte Anwendung des entschlüsselten Codes. Der Codeleser benötigt eine Spannungszuführung und ist relativ störanfällig im Vergleich zu den Codevergleichern und Logikelementen. Die Möglichkeit der Löschung und Neueingabe der Codes eröffnet nahezu zwangsläufig auch Möglichkeiten für die Entschlüsselung des Codes am Codegeber und am Codeleser.

Ziel der Erfindung ist die Erhöhung der Sicherheit der von codierten Schaltnetzwerken auszuführenden Öffnungs- oder Inbetriebnahmefunktionen.

Der Erfindung lag die Aufgabe zugrunde, ein elektronisch codiertes Sicherheitsschaltnetzwerk zu schaffen, das eine direkte Feststellung von Falschcodes und eine erhöhte Sicherheit der Öffnungs- oder Inbetriebnahmefunktionen vor ihnen aufweist, eine einmal erfolgte Schaltfunktion aufgrund eines Richtigcodes vor Kontaktschwierigkeiten sicher schützt, eine taktabhängige Codeübertragung als zusätzlichen Schutz gegen die unbefugte Anwendung des entschlüsselten Codes besitzt, auf einen Codeleser verzichtet und einen nicht löschbaren, fest programmierbaren Code im Codegeber und in den Codevergleichern aufweist.

Erfindungsgemäß wird diese Aufgabe mit den Merkmalen des kennzeichnenden Teils des Anspruchs 1 gelöst. Eine zweckmäßige Ausgestaltung dieser Merkmale erfährt der Gegenstand der Erfindung durch die Merkmale der Unteransprüche.

Die Erfindung soll nachstehend anhand eines Ausführungsbeispiels näher erläutert werden. In der zugehörigen Zeichnung zeigt:

Fig. 1 ein Blockschaltbild des Sicherheitsschaltnetzwerkes,

Fig. 2 die äußere Ausführung des Codegebers (a) und die Vorderansicht eines Zündschlosses als Steckeraufnahme (b),

Fig. 3 den Schaltungsaufbau des Codegebers,

Fig. 4 den Schaltungsaufbau des Codevergleichers und der Codeerkennungslogik,

Fig. 5 den Schaltungsaufbau der Schaltnetzwerk-Endstufe.

Als Ausführungsbeispiel wurde eine elektronisch codierte Wegfahrsperre für Kraftfahrzeuge gewählt. Diese läßt sich in folgende Funktionseinheiten bzw. -stufen aufgliedern (Fig. 1):

Der Codegeber 1 ist mit dem Eingang des Codevergleichers 2 verbunden. Der Codevergleicher ist aus dem Adressenvergleicher 3, dem Datenvergleicher 4 und dem mit diesen verbundenen Adressenspeicher 5 und Datenspeicher 6 zusammengesetzt, wobei der Codegeber 1 mit dem Eingang des Adressenvergleichers 3 und der Ausgang des Adressenvergleichers 3 mit dem Freigabeeingang des Datenvergleichers 4 verknüpft ist. Die Ausgänge der beiden Vergleichers 3; 4 sind an zwei der drei Eingänge der Codeerkennungslogik 7 angeschlossen, deren dritter Eingang mit dem Codegeber 1 in Verbindung steht. Die beiden ersten Eingänge sind die parallelen Eingänge der Richtigcodeerkennungsschaltung 8 und der digitalen Falschcodeerkennungsschaltung 9. Der dritte Eingang ist über den Impulsfolgeschalter 11 an den zweiten Eingang der analogen Falschcodeerkennungsschaltung 10 geführt, deren erster Eingang mit dem Ausgang des Datenvergleichers 4 verbunden ist. Der Richtigcodeerkennungsschaltung 8 ist eine eigene 12, den beiden Falschcodeerkennungsschaltungen 9; 10 eine gemeinsame Signalaufbereitungsstufe 13 nachge-

schaltet. Zwischen dem Ausgang der Stufe 13 und einem zweiten Eingang der Stufe 12 ist die Sperrzeitstufe 14 eingefügt. Die Ausgänge der Stufen 12; 13; 14 bilden die drei Eingänge der Schaltnetzwerk-Endstufe 18. Der Ausgang der Stufe 12 ist mit einem Eingang des Freigabeschalters 15 verbunden, an dessen zweitem Eingang die Freigabesperre 17 anliegt. Die Ausgänge der Stufen 13; 14 sind wahlweise an den Eingang des Sperrschalters 16 angeschlossen.

Der Codegeber 1 ist in dem als Gehäuse ausgebildeten Griff 19 des Zündschlüssels untergebracht, dessen metallischer Steckerteil (Bart) 20 in den Schließzylinder 21 eines Zündschlosses einführbar ist (Fig. 2). Der Anschlußkontakt A1 des Codegebers 1 für die positive Betriebsspannung ist mit einer isoliert im Griff 19 gelagerten Kontaktzunge 22 verbunden. Der Anschlußkontakt A2 für die Masse ist mit dem Bart 20 verbunden. Als Gegenkontakt zur Kontaktzunge 22 ist am Zündschloß ein Kontaktstreifen 23; E1 angeordnet, an dem die Betriebsspannung für den Codegeber 1 anliegt. Hauptbestandteil des Codegebers 1 ist der Codeschaltkreis IC1 mit Adressen (A)- und Daten (B)-Eingängen, die mit je einem Programmierbrückenspeicher PBSS1; PBSS2 verschaltet sind. Parallel zu den Betriebsspannungseingängen des Codeschaltkreises IC1 liegen ein Widerstand RS1 und ein Kondensator CS1, die die Systemtaktfrequenz bestimmen. Zwischen dem Datenausgang SA des Codeschaltkreises IC1 und einem der beiden Knotenpunkte des RC-Gliedes RS1; CS1 ist eine Diode DS1 eingefügt. Der Kondensator CS1 dient außerdem der Glättung der Betriebsspannung, die Diode DS1 hält die (negativen) Spannungsimpulse des Datenstromes von der Betriebsspannung fern (Fig. 3). Der Adressenvergleich 3 und der Datenvergleich 4 sind integrierte Schaltkreise IC2; IC3. Der Adressenspeicher 5 ist als Programmierbrückenspeicher PBSE1 und der Datenspeicher 6 als Programmierbrückenspeicher PBSE2 ausgeführt. Der Eingangskontakt E1 ist über eine Diode DE2 und einen Widerstand R4 auf einen vorgegebenen Spannungspegel gelegt. Zwischen dem Widerstand R4 und dem Eingang des Adressenvergleichers 3 ist ein Widerstand R5 geschaltet. Die Zenerdioden DE3 und DE4 dienen dem Überspannungsschutz, die Diode DE2 der Entkopplung des seriellen Datenstromes von der Gleichspannung und dem Schutz des Adressenvergleichers 3 vor Manipulationen mit positiven Spannungen am Eingangskontakt E1 (Fig. 4).

Die Richtigcodeerkennungsschaltung 8 ist aus dem NAND-Gatter 24, zwei seinen Eingängen e; f vorgeschalteten Negatoren 25; 26 und einem nachgeschalteten Negator 27 aufgebaut. Die dem Negator 27 folgende Signalaufbereitungsstufe 12 setzt sich aus dem NAND-Gatter 28, dem RC-Glied R14; C3 in der Anschlußleitung des ersten Eingangs g zum Negator 27 und dem Widerstand R15 zwischen der Betriebsspannung und dem zweiten Eingang h zusammen.

Die digitale Falschcodeerkennungsschaltung 9 besteht aus dem NAND-Gatter 29, dessen erster Eingang c direkt mit dem Ausgang $\overline{A=B}$ des Datenvergleichers 4 (IC3) und dessen zweiter Eingang d über den Negator 25 der Schaltung 8 mit dem Ausgang DA des Adressenvergleichers 3 (IC2) verknüpft ist. Die analoge Falschcodeerkennungsschaltung 10 ist als NAND-Gatter 30 ausgeführt. Der Impulsfolgeschalter 11 ist aus der Diode DE1, dem Kondensator C1, dem Widerstand R1, dem ersten Negator 31, dem RC-Dioden-Glied R2; R3; DE5; C2 und zwei in Reihe geschalteten Negatoren 32; 33 aufgebaut. Die Diode DE1 entkoppelt den seriellen Da-

tenstrom von der am Eingang des Impulsfolgeschalters 11 über den Widerstand R1 anliegenden Gleichspannung und schützt ihn (11) vor dem manipulierten Anlegen von positiven Spannungen. Die Aufladezeitkonstante des RC-Dioden-Gliedes R2; R3; DE5; C2 ist kleiner als die Aufladezeitkonstante des RC-Gliedes R14; C3 der Signalaufbereitungsstufe 12.

Die gemeinsame Signalaufbereitungsstufe 13 der Falschcodeerkennungsschaltungen 9; 10 besteht aus dem NAND-Gatter 34, dessen im Ruhezustand auf H-Pegel gehaltenen Eingänge x; y wahlweise über Programmierbrücken AE; DE an die Ausgänge der NAND-Gatter 30; 29 angeschlossen sind.

Die Sperrzeitstufe 14 setzt sich aus dem Transistor T1 in Kollektorschaltung, dem die Sperrzeit bestimmenden RC-Glied R21; C4 und dem Negator 35 zusammen, dessen Ausgang über die Programmierbrücke SPE an den zweiten Eingang h des NAND-Gatters 28 der Stufe 12 anschließbar ist.

Die Schaltnetzwerk-Endstufe 18 (Fig. 5) ist ganz speziell auf die Bedingungen eines Kraftfahrzeugs zugeschnitten. Sie kann für andere Anwendungen abweichend ausgeführt sein. Der Freigabeschalter 15 besitzt als Speicherschalter einen Trigger-Flip-Flop IC5 und als Endschalter einen nachgeschalteten Leistungstransistor T2 mit einem Relais A im Kollektorzweig. Der Setzeingang S des Flip-Flop IC5 ist an eine Reihenschaltung aus dem ersten Negator 36, dem NAND-Gatter 37 und dem zweiten Negator 38 angeschlossen. Dem Rücksetzeingang RD des Flip-Flop IC5 ist das NAND-Gatter 39 vorgeschaltet, dessen erster Eingang k über den Negator 40 an ein erstes RC-Glied RA2; CA1 und dessen zweiter Eingang l über den Negator 41 an ein zweites RC-Glied RA3; CA2 am Ausgang der Freigabesperre 17 angeschlossen ist. Der Kondensator CA1 liegt mit einem Kontakt an der Betriebsspannung, mit dem anderen Kontakt steht er außer mit dem Eingang des Negators 40 und dem Widerstand RA2 noch mit der Katode einer Diode DA1 in Verbindung. Die Diode DA1 bewirkt ein kurzzeitiges Entladen des Kondensators CA1 beim Abtrennen vom Bordnetz und damit ein Autoreset des Flip-Flop IC5. Der Ausgang des Negators 40 ist zusätzlich über die Diode DA3 in Sperrichtung mit dem zweiten Eingang j des NAND-Gatters 37 verbunden, wobei dieser Eingang j außerdem über den Widerstand RA1 an die Betriebsspannung 5P (5 V positive Spannung) und über eine andere Diode DA2 sowie einen vorgeschalteten Negator 42 an den Ausgang der Freigabesperre 17 angeschlossen ist. Die Freigabesperre 17 besteht aus dem RCR-Glied RA4; CA3; RA3 und dem nachfolgenden Negator 43. Die parallel geschaltete Zenerdiode DA4 schützt den Eingang des Negators 43 vor Überspannungen.

Der Sperrschalter 16 der Endstufe 18 weist den Leistungstransistor T3 mit dem Relais B im Kollektorzweig und im Basiszweig zwei Programmierbrücken BFK; BFL für den wahlweisen Anschluß an die Signalaufbereitungsstufe 13 oder die Sperrzeitstufe 14 auf. Die Relaiskontakte a1; a2, a3 des Freigabeschalters 15 sind Arbeitskontakte, die Relaiskontakte b1; b2; b3 dagegen Ruhekkontakte im Zünd- und Anlasserstromkreis sowie in einem Stromkreis für den Benzinpumpenmotor.

Alle Betriebsspannungszuführungen 5P sind an den Ausgang des Festspannungsreglers IC4 angeschlossen, dessen Eingang 12P (12 V positive Spannung) über eine Schutzdiode DA7 mit dem Pluspol der Autobatterie verbunden ist.

Das beschriebene Sicherheitsschaltnetzwerk besitzt

folgende Wirkungsweise:

Beim Einstecken des Zündschlüssels in den Schließzylinder 21 wird sofort eine leitende Verbindung zwischen dem Anschlußkontakt A2 und dem Eingangskontakt E2 (Masse) hergestellt. Durch Drehen des Schlüssels in die Zündstellung kommen die Kontaktzunge 22 und der Kontaktstreifen 23 in Berührung, wodurch die Verbindung zwischen dem Anschlußkontakt A1 und dem Eingangskontakt E1 zustande kommt. Der Codeschaltkreis IC1 und die Speicher PBSS1; PBSS2 erhalten Betriebsspannung, wodurch automatisch das gespeicherte, aus Adressen- und Datenteil bestehende Codewort als serielle Datenfolge in einem definierten Takt über DE2 und R5 in den Adressenvergleich 3 (IC2) eingegeben wird. Wird dieses als systemgerecht und damit als Echtt- bzw. Richtigcode erkannt, wird das Flip-Flop IC5 gesetzt, wodurch der Leistungstransistor T2 Strom führt und das Relais A seine Arbeitskontakte a1; a2; a3 in den genannten Stromkreisen schließt. Jetzt startet das Fahrzeug. Kontaktschwierigkeiten bei der Codeübertragung während des Betriebes des Kfz haben wegen der Speicherung des Schaltzustandes im Flip-Flop IC5 keinen Einfluß.

Bei Übereinstimmung des Adressenteils des Codewortes mit der Adresse A1—A10 des Programmierbrückenspeichers PBSE1 schaltet der Datenausgang DA des IC2 von H- auf L-Pegel, der den IC3 für den Vergleich der an seinen Eingängen A0—A7 anliegenden Daten mit denen an seinen Eingängen B0—B7 freischaltet. Die Widerstände R6—R13 sorgen für eindeutige Pegelverhältnisse bei offenen Programmierbrückenanschlüssen am Speicher PBSE2 (L-Pegel). Bei Datenübereinstimmung nimmt der Ausgang des IC3 L-Pegel an.

Die Schaltvorgänge und -zustände aller Stufen des Schaltnetzwerkes lassen sich durch die Angabe der Pegel an den einzelnen Stellen im Schaltbild verdeutlichen. Dabei kennzeichnen in Klammern gesetzte Pegelangaben — (H) oder (L) — den Zustand ohne Adressen- und/oder Datenübereinstimmung bzw. den Zustand vor der Codeerkennung und die Pegelangaben ohne Klammern — H oder L — den Zustand bei bzw. nach der Codeerkennung. Wichtig für das Verständnis der Vorgänge ist der Umstand, daß die NAND-Gatter nur reagieren, wenn schon ein Eingang auf H-Pegel liegt.

Ein Richtigcode wird am Ausgang R des NAND-Gatters 28 mit einem H-L Pegelsprung signalisiert, wodurch die Leuchtdiode LD3 aufleuchtet.

Ein Falschcode macht sich durch einen L-H Pegelsprung am Ausgang FK des NAND-Gatters 34 bemerkbar, wodurch die Leuchtdiode LD1 aufleuchtet. Gleichzeitig erhält der Transistor T1 über den Widerstand R19 Basisspannung und steuert durch. Der Kondensator C4 wird über den Strombegrenzungswiderstand R20 schnell aufgeladen. Der Eingang des Negators 35 erhält so H-Pegel, wodurch sein Ausgang FL in den L-Pegel übergeht. Bei geschlossener Programmierbrücke SPE geht der Eingang h des NAND-Gatters 28 ebenfalls auf L-Pegel. Die Signalaufbereitungsstufe 12 ist somit für eine durch die Entladezeitkonstante des RC-Gliedes R21; C4 bestimmte Zeit, z. B. 3 Minuten, für die Signalverarbeitung des Richtigcodes gesperrt. In dieser Zeit wären auch Startversuche mit dem richtigen Zündschlüssel erfolglos. Bei erneuten Versuchen mit einem Falschcode innerhalb der Sperrzeit verlängert sich diese in Abhängigkeit vom Beginn des Versuchs. Das erklärt sich dadurch, daß der Kondensator C4 erneut geladen wird, was die Entladung und die Aufhebung der Sperre verhindert.

Die gegenüber dem RC-Dioden-Glied R2; R3; DE5; C2 größere Aufladezeitkonstante des RC-Gliedes R14; C3 bewirkt, daß die Auswertzeit für den Richtigcode länger ist als für den Falschcode. Ein Falschcode wird daher eher erfaßt und in Sperrsignale umgewandelt. Manipulationen am Codevergleicher 3 werden so erheblich erschwert.

Die analoge Falschcodeerkennungsschaltung 10 spricht schon bei fehlender Adressenübereinstimmung an. Sie arbeitet mit einem Impulsfolgeschalter 11 zusammen, der im Prinzip ein Integrator von H-L Pegelsprüngen mit angeschlossenem Schwellenschalter (32; 33) ist. Er reagiert sowohl bei Richtig- als auch bei Falschcode.

Das Anlegen der Bordspannung ZS/12P bei Zündfreigabe an die Freigabesperre 17 bewirkt wegen der relativ langsamen Aufladung des Kondensators CA3 eine verzögerte Pegeländerung von L auf H am Eingang j des NAND-Gatters 37. In dieser Zeit kann eine Pegeländerung von H auf L am Eingang R infolge Anliegens eines Richtigcodes zu keinem Setzen des Flip-Flop IC5 führen. Auch beim Anschluß der Betriebsspannung 5P wird das NAND-Gatter 37 kurzzeitig blockiert. Dafür sorgt die relativ langsame Aufladung des Kondensators CA1.

Im Betriebszustand befinden sich beide Eingänge k; l des NAND-Gatters 39 auf H-Pegel. Am Gatterausgang und somit am Rücksetzeingang RD des Flip-Flop IC5 liegt L-Pegel an. Beim Ausschalten der Zündung kommt es am Ausgang des Negators 41 zu einem kurzen H-L Pegelsprung, was durch das NAND-Gatter 39 negiert einen kurzen L-H Pegelsprung am Rücksetzeingang RD bewirkt. Die Folge ist ein Rücksetzen des Flip-Flop IC5. Sein Q-Ausgang liegt auf L-Pegel, das Relais A fällt ab und öffnet seine Kontakte a1; a2; a3, die Stromkreise für die Zündung, den Anlasser und den Benzinpumpenmotor werden unterbrochen.

Patentansprüche

1. Elektronisches Sicherheitsschaltnetzwerk mit einem als Steckereinheit ausgeführten, einen zweiteiligen Code aufweisenden Codegeber, einer Steckeraufnahme, einem Codevergleicher, einem Codespeicher, einer Richtigcodeerkennungsschaltung und einer Netzwerk-Endstufe mit Schaltern für die zu sichernden Öffnungs- oder Inbetriebnahmefunktionen, **dadurch gekennzeichnet**, daß der Codegeber (1) eine Systemtaktfrequenz aufweist und ausgangsseitig mittels Entkopplungselementen (DS1; DE2) über die Betriebsspannungszuleitung mit dem Codevergleicher (2) verbunden ist, die Steckeraufnahme (21) nur die Kontakte (E1; E2) für die Betriebsspannungsversorgung aufweist, der Codevergleicher (2) aus einem separaten Adressenvergleich (3) und einem separaten Datenvergleich (4) mit angeschlossenen Adressen- und Datenspeicher (5; 6) zusammengesetzt ist, wobei der Codegeber (1) mit dem Eingang des Adressenvergleichers (3) und dieser (3) ausgangsseitig mit dem Freigabeeingang (E) des Datenvergleichers (4) verknüpft ist, zusätzlich eine digitale Falschcodeerkennungsschaltung (9) vorgesehen ist, wobei die Eingänge der Richtigcodeerkennungsschaltung (8) und der digitalen Falschcodeerkennungsschaltung (9) jeweils mit den Ausgängen (DA; A=B) des Adressenvergleichers (3) und des Datenvergleichers (4) verbunden sind, weiterhin eine analoge Falschcodeerkennungsschaltung (10) vorgesehen ist, deren

einer Eingang mit dem Ausgang ($\overline{A=B}$) des Datenvergleichers (4) und deren anderer Eingang über einen Impulsfolgeschalter (11) mit dem Codegeber (1) in Verbindung steht, der Richtigcodeerkennungsschaltung (8) eine eigene (12) und den Falschcodeerkennungsschaltungen (9; 10) eine gemeinsame Signalaufbereitungsstufe (13) nachgeschaltet ist, die Signalaufbereitungsstufe (12) der Richtigcodeerkennungsschaltung (8) und der Impulsfolgeschalter (11) je ein Verzögerungsglied (R14-C3; R2-C2) enthalten, wobei die Verzögerung der Signalaufbereitungsstufe (12) größer als die Verzögerung des Impulsfolgeschalters (11) ist, zwischen dem Ausgang (FK) der gemeinsamen Signalaufbereitungsstufe (13) und einem zweiten Eingang der separaten Signalaufbereitungsstufe (12) eine Sperrzeitstufe (14) eingefügt ist, deren Sperrzeit größer als die Erkennungs- und Aufbereitungszeit des Richtigcodes ist, der Ausgang (FL) des Sperrzeitalters (14) außerdem wahlweise anstelle des Ausgangs (FK) der gemeinsamen Signalaufbereitungsstufe (13) an einen Sperrschalter (16) der Schaltnetzwerk-Endstufe (18) anschließbar ist, der Ausgang (R) der separaten Signalaufbereitungsstufe (12) an einen Freigabeschalter (15) der Schaltnetzwerk-Endstufe (18) geführt ist und der Freigabeschalter (15) einen bistabilen Schalter (IC5) einschließt.

2. Elektronisches Sicherheitsschaltnetzwerk nach Anspruch 1, dadurch gekennzeichnet, daß Bestandteil des Codegebers (1) ein Codeschaltkreis (IC1) mit Adressen (A)- und Dateneingängen (B) ist, die mit je einem Programmierbrückenspeicher (PBSS1; PBSS2) verbunden sind, die Systemtaktfrequenz durch ein RC-Glied (RS1; CS1) parallel zu den Betriebsspannungseingängen des Codeschaltkreises (IC1) festgelegt ist und eine Diode (DS1) zwischen dem mit dem Datenausgang (SA) des Codeschaltkreises (IC1) verknüpften Anschlußkontakt (A1) und dem einen Knotenpunkt des RC-Gliedes (RS1; CS1) eingefügt ist.

3. Elektronisches Sicherheitsschaltnetzwerk nach Anspruch 1 und 2, dadurch gekennzeichnet, daß der Adressenvergleicher (3) und der Datenvergleicher (4) als integrierte Schaltkreise (IC2; IC3) und der Adressenspeicher (5) und der Datenspeicher (6) als Programmierbrückensysteme (PBSE1; PBSE2) ausgeführt sind.

4. Elektronisches Sicherheitsschaltnetzwerk nach Anspruch 1 bis 3, dadurch gekennzeichnet, daß die Richtigcodeerkennungsschaltung (8) aus einem NAND-Gatter (24), zwei seinen Eingängen (e; f) vorgeschalteten Negatoren (25; 26) und einem nachgeschalteten Negator (27) aufgebaut ist und die angeschlossene Signalaufbereitungsstufe (12) aus einem NAND-Gatter (28), einem RC-Glied (R14; C3) in der Anschlußleitung zu dem einen Eingang (g) und einem Widerstand (R15) zwischen dem anderen Eingang (h) und der Betriebsspannung zusammengesetzt ist.

5. Elektronisches Sicherheitsschaltnetzwerk nach Anspruch 1 bis 4, dadurch gekennzeichnet, daß die digitale Falschcodeerkennungsschaltung (9) aus einem NAND-Gatter (29) besteht, dessen erster Eingang (c) direkt mit dem Ausgang ($\overline{A=B}$) des Datenvergleichers (4; IC3) und dessen zweiter Eingang (d) über einen Negator (25) der Richtigcodeerkennungsschaltung (8) mit dem Ausgang (DA)

des Adressenvergleichers (3; IC2) verknüpft ist.

6. Elektronisches Sicherheitsschaltnetzwerk nach Anspruch 1 bis 5, dadurch gekennzeichnet, daß die analoge Falschcodeerkennungsschaltung (10) als NAND-Gatter (30) ausgeführt ist und der Impulsfolgeschalter (11) aus einer Diode (DE1), einem Kondensator (C1), einem ersten Negator (31), einem RC-Dioden-Glied (R2; R3; DE5; C2) und zwei in Reihe geschalteten Negatoren (32; 33) aufgebaut ist.

7. Elektronisches Sicherheitsschaltnetzwerk nach Anspruch 1 bis 6, dadurch gekennzeichnet, daß die gemeinsame Signalaufbereitungsstufe (13) der Falschcodeerkennungsschaltungen (9; 10) aus einem NAND-Gatter (34) besteht, dessen im Ruhezustand auf H-Pegel gehaltene Eingänge (x; y) wahlweise über Programmierbrücken (AE; DE) an die Ausgänge der NAND-Gatter (29; 30) angeschlossen sind.

8. Elektronisches Sicherheitsschaltnetzwerk nach Anspruch 1 bis 7, dadurch gekennzeichnet, daß die Sperrzeitstufe (14) aus einem Transistor (T1) in Kollektorschaltung, einem die Sperrzeit bestimmenden RC-Glied (R21; C4) und einem Negator (35) besteht, dessen Ausgang über eine Programmierbrücke (SPE) an den zweiten Eingang (h) des NAND-Gatters (28) der separaten Signalaufbereitungsstufe (12) anschließbar ist.

9. Elektronisches Sicherheitsschaltnetzwerk nach Anspruch 1 bis 8, dadurch gekennzeichnet, daß der Freigabeschalter (15) der Schaltnetzwerk-Endstufe (18) als bistabilen Schalter einen Trigger-Flip-Flop (IC5) und als Endscharter einen nachgeschalteten Transistor (T2) mit einem Relais (A) im Kollektorzweig aufweist, der Setzeingang (S) des Flip-Flop (IC5) an eine Reihenschaltung aus einem ersten Negator (36), einem NAND-Gatter (37) und einem zweiten Negator (38) angeschlossen ist, dem Rücksetzeingang (RD) des Flip-Flop (IC5) ein NAND-Gatter (39) vorgeschaltet ist, dessen erster Eingang (k) über einen ersten Negator (40) mit einem ersten RC-Glied (CA1; RA2) und dessen zweiter Eingang (l) über einen zweiten Negator (41) mit einem zweiten RC-Glied (RA3; CA2) am Ausgang einer Freigabesperre (17) in Verbindung steht, der Kondensator (CA1) des ersten RC-Gliedes mit einem Kontakt an die Betriebsspannung geführt ist, der Ausgang des ersten Negators (40) zusätzlich über eine Diode (DA3) in Sperrrichtung mit dem zweiten Eingang (j) des dem Setzeingang (S) zugeordneten NAND-Gatters (37) verbunden ist, wobei dieser Eingang (j) außerdem über einen Widerstand (RA1) an die Betriebsspannung (5P) und über eine andere Diode (DA2) an den Ausgang der Freigabesperre (17) angeschlossen ist.

10. Elektronisches Sicherheitsschaltnetzwerk nach Anspruch 1 bis 9, dadurch gekennzeichnet, daß die Freigabesperre (17) aus RCR-Glied (RA4; CA3; RA5), einer Zenerdiode (DA4) und einem nachgeschalteten Negator (43) besteht.

11. Elektronisches Sicherheitsschaltnetzwerk nach Anspruch 1 bis 10, dadurch gekennzeichnet, daß der Sperrschalter (16) der Endstufe (18) einen Transistor (T3) im Kollektorzweig und im Basiszweig zwei Programmierbrücken (BFK; BFL) zum wahlweisen Anschluß an den Ausgang (FK) der Signalaufbereitungsstufe (13) der Falschcodeerkennungsschaltungen (9; 10) oder an den Ausgang (FL) der

Sperrzeitstufe (14) aufweist.

Hierzu 4 Seite(n) Zeichnungen

5

10

15

20

25

30

35

40

45

50

55

60

65

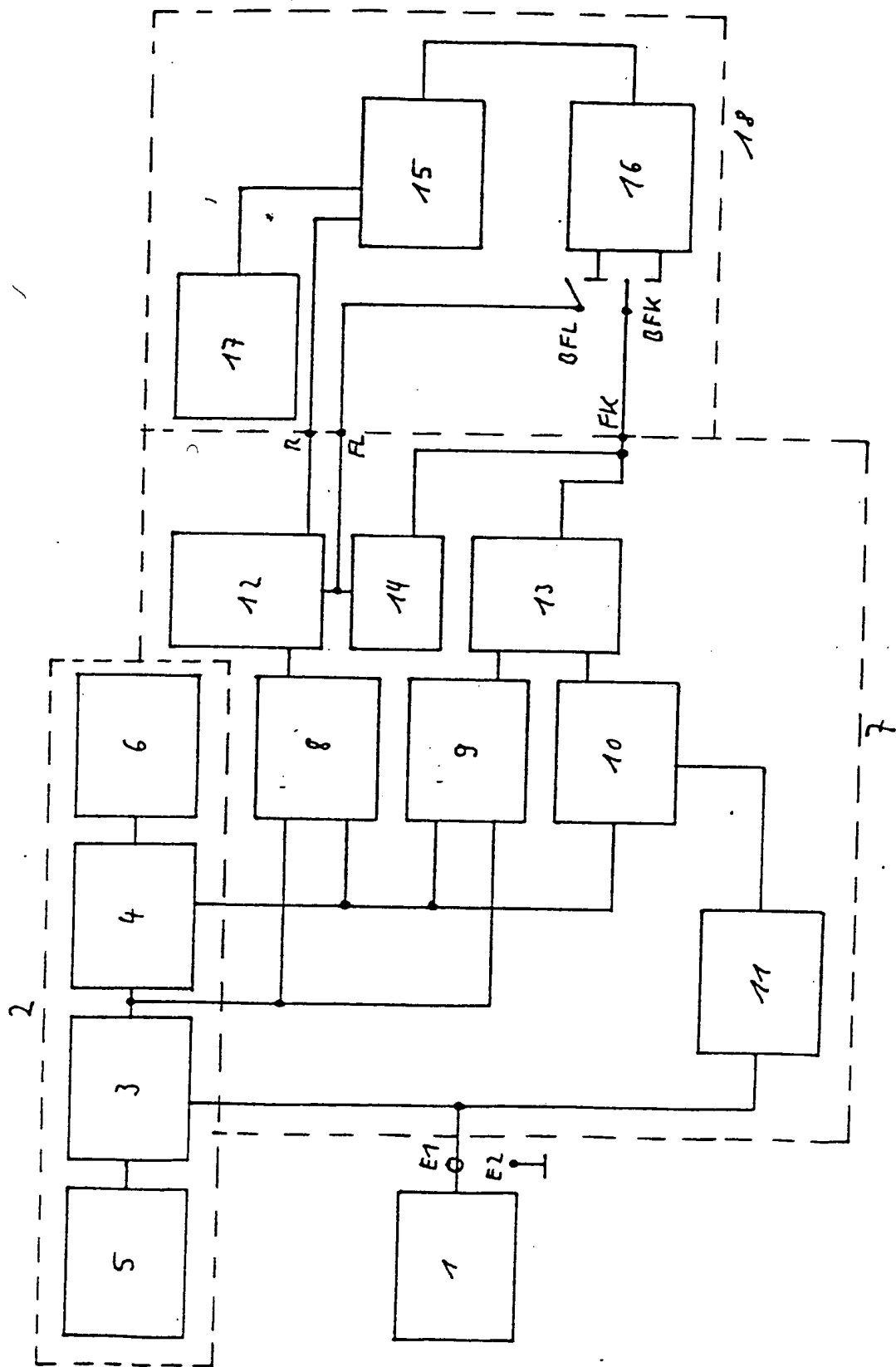


Fig. 1

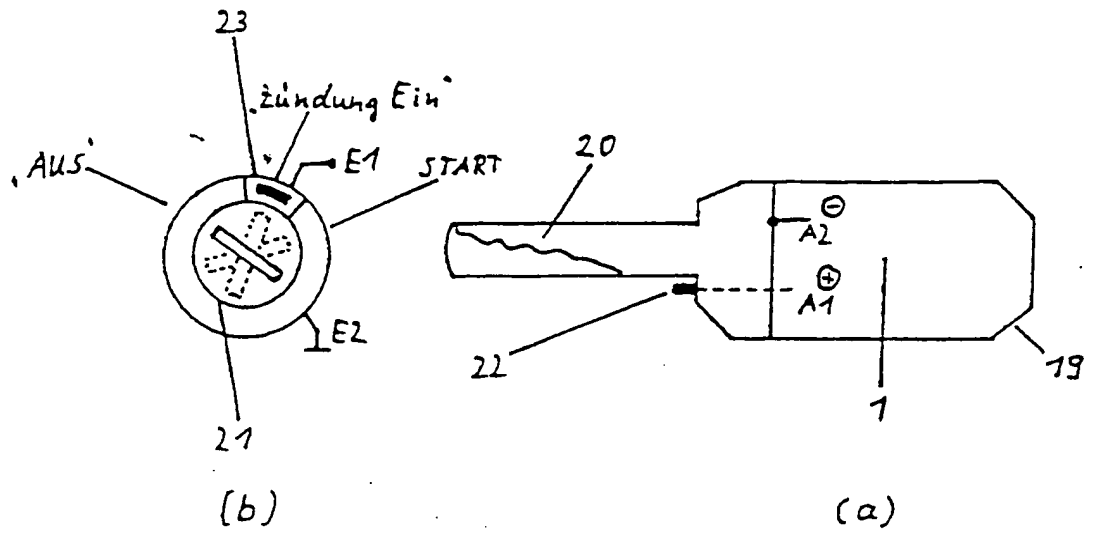


Fig. 2

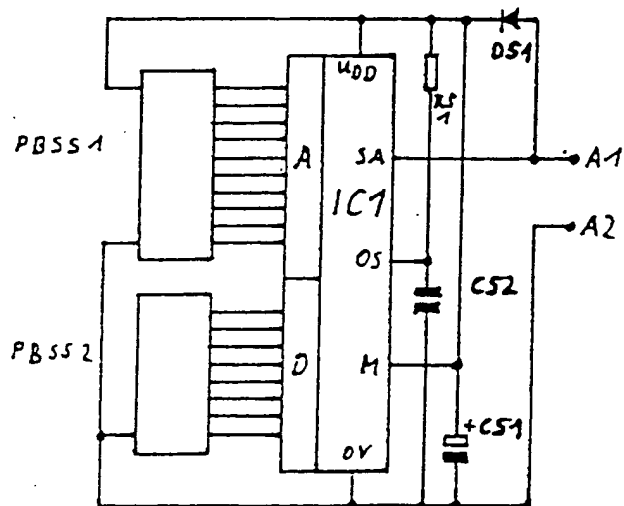


Fig. 3

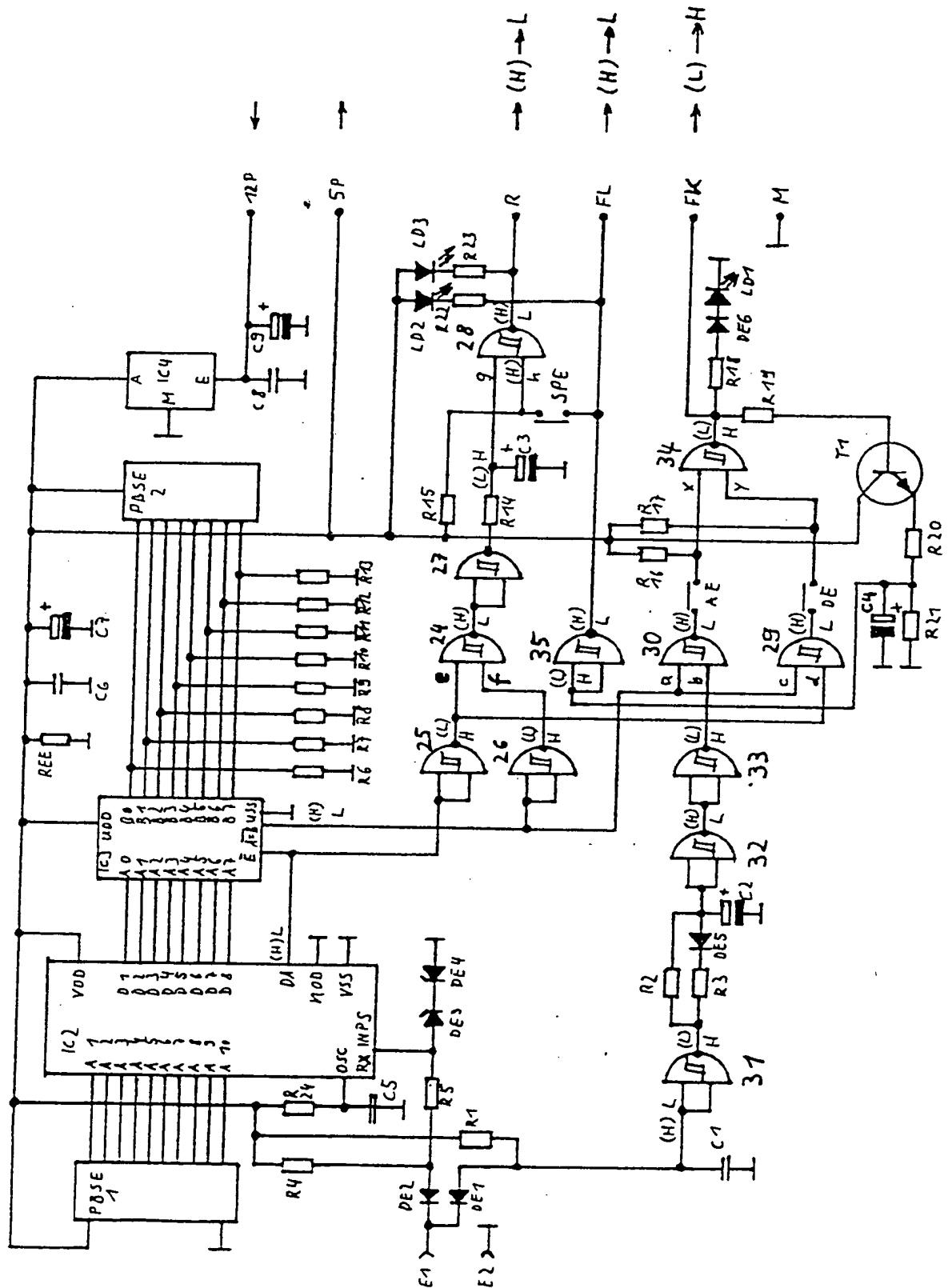


Fig. 4

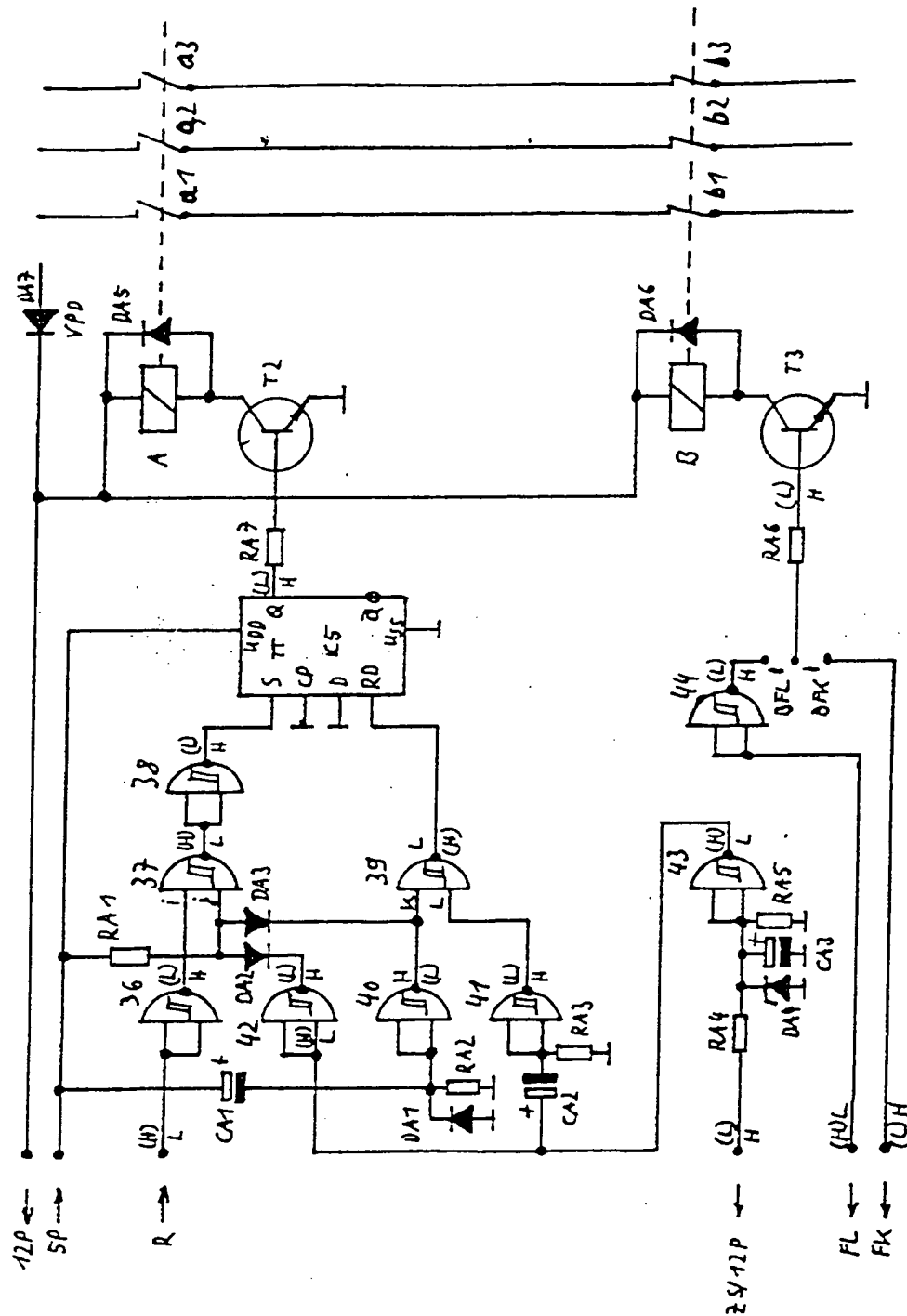


Fig. 5